


## Chapter 32

# Protection to Personal Data Using Decentralizing Privacy of Blockchain.

**Vilas Baburao Khedekar**

 <https://orcid.org/0000-0003-4229-1937>

*VIT University, India*

**Shruti Sangmesh Hiremath**

*Jayawantrao Sawant College of Engineering, India*

**Prashant Madhav Sonawane**

*Jayawantrao Sawant College of Engineering, India*

**Dharmendra Singh Rajput**

*VIT University, India*

### ABSTRACT

*In today's world, we deal with various online services, where each person deals with various technologies. These technologies are made for people to make our access to the new world easily. There is a tremendous use of online applications, websites which require large storage. Large data is handled by the online systems. The collection of data in the whole world is about 20% in the last few years. The data is captured from the user, controlled by the systems, and operations are performed on data. It requires more system accuracy and protection to personal data. But the person does not know about the data, where and how it is used where it is stored or whether the data is handled by some organisations for their own use or data is been hacked by another person. This chapter explores protection of data using the decentralized privacy of blockchain.*

DOI: 10.4018/978-1-6684-7132-6.ch032

## **INTRODUCTION**

In today's world we deal with various online services, where each person deals with various technologies. These technologies are made for people to make our access to new world easily. There is tremendous use of online applications, websites which require large storage. Large data is handled by the online systems. The collection of data in whole world is about 20% in last few years ("Big data, for better or worse: 90% of world's data generated over last two years," 2013). The data is captured from user, controlled by the systems and operations are performed on data. It requires more system accuracy and protection to personal data.

Ex. Email, WhatsApp, Instagram, Facebook, Bank transactions, Real-time estate etc. But the person is unknown about the data, where and how it is used where it is stored or whether the data is handled by some organisations for their own use or data is been hacked by other person (Zyskind & Pentland, 2015). Since the protection towards the personal data is been decreasing day by day. Example- Facebook one of the huge online social network collected 300 petabytes of user data during its inception (PB, n.d.). These leads to illegally accessing personal data for their own purpose without having rights on it.

## **WHAT IS THE PERSONAL DATA?**

Every person deals with various applications nowadays, where each website or application needs authentication of user. He has must create a user id and set password to access the application. He has a unique identity .He keeps his access details up to him, where the data contains login details which he wants to keep private .Personal data is defined as the individual information which is used to identifying a person identity from others . These details may be used to trace the person .The name, identity number, account details, birth date, mothers name, biometrics and various information regarding website access, banking details and medical details is related to an individual. One of these details are enough to identify an individual. These details are not shared with others .These data is kept hidden from public. Only that person can handle or deal with his data .The data is kept private .The data is kept secured .

## **The Privacy Problem**

In various fields, the services deploy applications for users to install. All these applications collect high resolution of personal data. The user is unknown about this process. The person is providing all the data to the applications and allow the applications to deal with his personal data on the system. The application may misuse the authentication details of the user. This results in tracing the user details whenever required . Even the hackers can easily trap the system and get access of the personal details of the system .In agriculture environment the third parties involve between farmers and customers to deal the transaction .This leads to get advantage over the other .The broker earns more profit than farmer.

## **What Is Blockchain?**

Blockchain is a decentralised, distributed, public ledger. Blockchain is defined as collection of blocks. Block is the smallest unit of blockchain which records recent transactions. Every transactions are grouped and stored on a public ledger (*b-money*, 1998). In blockchain, the first block is called as genesis block.

16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:  
[www.igi-global.com/chapter/protection-to-personal-data-using-decentralizing-privacy-of-blockchain/310469](http://www.igi-global.com/chapter/protection-to-personal-data-using-decentralizing-privacy-of-blockchain/310469)

## Related Content

---

### Generative AI-Enabled IoT Applications for Smart Cities: Unleashing Innovation and Paving the Way for the Future

Anupriya Sharma Ghai, Kapil Ghai and Gulsun Kurubacak Cakir (2024). *Secure and Intelligent IoT-Enabled Smart Cities* (pp. 222-238).

[www.irma-international.org/chapter/generative-ai-enabled-iot-applications-for-smart-cities/343452](http://www.irma-international.org/chapter/generative-ai-enabled-iot-applications-for-smart-cities/343452)

### An International Overview of the Electronic Financial System and the Risks Related to It

Tatiana Dnescu, Alexandra Boto and Ionica Oncioiu (2019). *Network Security and Its Impact on Business Strategy* (pp. 44-59).

[www.irma-international.org/chapter/an-international-overview-of-the-electronic-financial-system-and-the-risks-related-to-it/224863](http://www.irma-international.org/chapter/an-international-overview-of-the-electronic-financial-system-and-the-risks-related-to-it/224863)

### An Approach for Intentional Modeling of Web Services Security Risk Assessment

C. Misra Subhas, Kumar Vinod and Kumar Uma (2010). *Web Services Security Development and Architecture: Theoretical and Practical Issues* (pp. 295-308).

[www.irma-international.org/chapter/approach-intentional-modeling-web-services/40598](http://www.irma-international.org/chapter/approach-intentional-modeling-web-services/40598)

### Verifiable Authentication and Issuance of Academic Certificates Using Permissioned Blockchain Network

Erukala Suresh Babu, B. K. N. Srinivasarao, Ilaiyah Kavati and Mekala Srinivasa Rao (2022). *International Journal of Information Security and Privacy* (pp. 1-24).

[www.irma-international.org/article/verifiable-authentication-and-issuance-of-academic-certificates-using-permissioned-blockchain-network/284052](http://www.irma-international.org/article/verifiable-authentication-and-issuance-of-academic-certificates-using-permissioned-blockchain-network/284052)

### Identification of Cryptographic Vulnerability and Malware Detection in Android

Anjali Kumawat, Anil Kumar Sharma and Sunita Kumawat (2017). *International Journal of Information Security and Privacy* (pp. 15-28).

[www.irma-international.org/article/identification-of-cryptographic-vulnerability-and-malware-detection-in-android/181545](http://www.irma-international.org/article/identification-of-cryptographic-vulnerability-and-malware-detection-in-android/181545)